Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn

nytimes.com/2018/02/13/us/politics/russia-sees-midterm-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html

By Matthew Rosenberg , Charlie Savage and Michael Wines February 13, 2018

WASHINGTON — Russia is already meddling in the midterm elections this year, the top American intelligence officials said on Tuesday, warning that Moscow is using a digital strategy to worsen the country's political and social divisions.

Russia is using fake accounts on social media — many of them bots — to spread disinformation, the officials said. European elections are being targeted, too, and the attacks were not likely to end this year, they warned.

"We expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespeople and other means of influence to try to exacerbate social and political fissures in the United States," Dan Coats, the director of national intelligence, told the Senate Intelligence Committee at its annual hearing on worldwide threats.

Mr. Coats and the other intelligence chiefs laid out a pair of central challenges for the United States: contending with the flow of Russian misinformation and shoring up the defenses of electoral systems, which are run by individual states and were seen as highly vulnerable in 2016.

“There should be no doubt that Russia perceives its past efforts as successful and views the 2018 U.S. midterm elections as a potential target for Russian influence operations,” said Mr. Coats, testifying alongside Mike Pompeo, the C.I.A. director; Christopher A. Wray, the F.B.I. director; and other leading intelligence officials.

“Throughout the entire community, we have not seen any evidence of any significant change from last year,” Mr. Coats said.

The warnings were striking in their contrast to President Trump’s public comments. He has mocked the very notion of Russian meddling in the last election and lashed out at those who suggested otherwise.

Mr. Trump has not directed his intelligence officials to specifically combat Russian interference, they said. But Mr. Pompeo said that the president has made clear that the C.I.A. has “an obligation, from the foreign intelligence perspective, to do everything we can to make sure there’s a deep and thorough understanding of every threat, including threats from Russia.”

Russia appears eager to spread information — real and fake — that deepens political divisions. Bot armies promoted partisan causes on social media, including the recent push to release a Republican congressional memo critical of law enforcement officials.

The bots have also sought to portray the F.B.I. and Justice Department as infected by partisan bias, said Senator Mark Warner of Virginia, the top Democrat on the intelligence committee.

“Other threats to our institutions come from right here at home,” he said. “There have been some, aided and abetted by Russian internet bots and trolls, who have attacked the basic integrity of the F.B.I. and the Justice Department. This is a dangerous trend.”

Russia does not, however, appear to be trying to penetrate voting machines or Americans’ ballots, United States officials said.

“While scanning and probing of networks happens across the internet every day, we have not seen specific or credible evidence of Russian attempts to infiltrate state election infrastructure like we saw in 2016,” Jeanette Manfra, the chief cybersecurity official at the Department of Homeland Security, said in an interview last week.

Right now, Mr. Pompeo said, Russia is trying to focus on what are known as influence operations — using social media and other platforms to spread favorable messages — not hacking.

“The things we have seen Russia doing to date are mostly focused on information types of warfare,” he said.

Intelligence officials and election-security experts have said both the states and federal agencies have made significant progress in addressing voting system vulnerabilities since 2016, when state-level officials could not even be warned of attacks because they lacked the necessary security clearances.

The intelligence community was focused on gathering information about potential attacks and then sharing it with local and state election officials, Mr. Coats said during the hearing.

Mr. Coats called Moscow's meddling "pervasive."

"The Russians have a strategy that goes well beyond what is happening in the United States," he said. "While they have historically tried to do these types of things, clearly in 2016 they upped their game. They took advantage, a sophisticated advantage of social media. They are doing that not only in the United States but doing it throughout Europe and perhaps elsewhere."

Mr. Pompeo was also asked about reports last week by The New York Times and The Intercept that American intelligence agencies spent months negotiating with a Russian who said he could sell stolen American cyberweapons and that the deal would include purportedly compromising material on Mr. Trump. The negotiations were conducted through an American businessman who lives in Europe and served as a cutout for American intelligence agencies.

Mr. Pompeo called the reporting "atrocious, ridiculous and inaccurate" and said the C.I.A. had not paid the Russian. The Times, citing American and European intelligence officials, said only that American spies had paid the Russian $100,000 for the cyberweapons using an indirect channel. Those weapons were never delivered. The Russian did provide information on Mr. Trump, which intelligence agencies refused to accept and remains with the American businessman.

"Our story was based on numerous interviews, a review of communications and other evidence. We stand by it," said Dean Baquet, the executive editor of The Times.

Mr. Pompeo did appear to acknowledge the operation itself, saying that "the information that we were working to try and retrieve was information we believed might well have been stolen from the U.S. government."

He and the other intelligence chiefs, including Adm. Michael S. Rogers, the departing director of the National Security Agency, also addressed the slew of other threats they see facing the United States. They cited North Korea's nuclear program, Islamist militants in the Middle East and even illicit drug trafficking, especially the smuggling of cheaply made fentanyl, a powerful opioid responsible for thousands of deaths each year.

But as has been the case for years, the intelligence leaders presented cyberactivities of rival nations and rogue groups as the foremost threat facing the United States. They warned that such risks were likely to only grow, citing China, Iran, North Korea and Russia, along with militant groups and criminal networks, as the main agitators.

To ease the flow of information, the Department of Homeland Security is trying to get at least one election official in each state a security clearance. To date, 21 officials in 20 states received at least interim "secret"-level clearances, Ms. Manfra said in the interview.

The federal government is also working to provide states with enhanced online security “to ensure the American people that their vote is sanctioned and well and not manipulated in any way,” Mr. Coats said.

Homeland Security has added 32 states and 31 local governments to a system that scans internet-connected systems in the federal government every night for vulnerabilities, offering weekly reports and fixes to any issues they find, Ms. Manfra said.

Specialists also spend weeks auditing cyberdefense systems in both federal agencies and state elections offices, and last month, the department decided to prioritize requests for the latter to ensure that they get done swiftly, she added.

Virtually every state is taking steps to harden voter databases and election equipment against outside attacks and to strengthen postelection audits. When the National Association of Secretaries of State holds its winter meeting this weekend in Washington, half of the sessions will be devoted wholly or in part to election security.

New standards for voting equipment were approved last fall that will effectively require manufacturers to include several security improvements in new devices. States are moving to scrap voting machines that do not generate an auditable paper ballot as well as an electronic one; Virginia has decertified most of its devices, Pennsylvania has declared that all new devices will produce paper ballots, and Georgia — a state whose outdated equipment produces only electronic voting records — has set up a pilot program to move to paper.

But a host of problems remains. Roughly one-fifth of the country lacks paper ballots, and replacing digital-only machines costs millions of dollars. Federal legislation that would allot funds to speed up the conversion to paper is crawling through Congress.

Many experts, meanwhile, believe that Russian meddling in the presidential race was but a foretaste of what is to come — not just from the Kremlin, but also from other hostile states and private actors.

“Russia learned a lot last year in what really, I think, can be seen as a series of probing attacks,” Douglas Lute, a retired Army lieutenant general, deputy national security adviser to President George W. Bush and ambassador to NATO under President Barack Obama, said in an interview. “I think we should expect that they learned and they’re going to come back in a much more sophisticated way.”